

**Regolamento (UE) 2016/679**  
del Parlamento europeo e del Consiglio, del 27 aprile 2016  
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

**Regolamento interno per l'utilizzo dei sistemi e strumenti informatici  
all'interno di I.C. MIRTO CROSIA**

PROT. N 3333

CROSIA 11/06/2018

**Indice**

**Premessa**

1. Entrata in vigore del Regolamento e pubblicità
2. Campo di applicazione del Regolamento
3. Utilizzo del Personal Computer
4. Gestione e assegnazione delle credenziali di autenticazione
5. Utilizzo della rete
6. Utilizzo di dispositivi elettronici
7. Utilizzo e conservazione dei supporti rimovibili
8. Uso della posta elettronica
9. Navigazione in Internet
10. Protezione antivirus
11. Partecipazione a social media
12. Osservanza delle disposizioni in materia di Privacy
13. Accesso ai dati trattati dall'utente
14. Sistema di controlli gradualità
15. Sanzioni
16. Aggiornamento e revisione

**Premessa**

ISTITUTO COMPRENSIVO MIRTO CROSIA (di seguito "Titolare") ha disposto che al proprio interno venga osservato il presente Regolamento.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone il Titolare e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine del Titolare stesso.

Peraltro, anche lo sviluppo delle reti sociali on-line incide, direttamente o indirettamente, sulle attività del Titolare, sulla sua immagine e sulle relazioni commerciali instaurate. Infatti, l'uso dei *social media*, quali Facebook™, Twitter™, LinkedIn™, dei blog e dei forum, anche professionali, costituisce un efficace strumento di condivisione di contenuti (testi, immagini, video) da parte degli utenti e, allo stesso tempo, un'evidente opportunità per il titolare, in particolare in ambito commerciale e di marketing. Risulta però necessario che, al fine di evitare il sorgere di rischi derivanti dalla presenza della denominazione del titolare e/o di altri riferimenti ad esso riconducibili, eventualmente solo indiretta, sui *social media*, si tenga pure conto di questo preciso aspetto nel presente Regolamento.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il Titolare ha adottato un Regolamento interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico. Il Regolamento svolge anche la funzione di informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che vengono effettuati, e delle modalità adottate.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento Europeo sulla protezione dei dati (da ora in poi GDPR 2016/679), nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del predetto regolamento, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4-3° comma dello Statuto dei lavoratori.

Considerato inoltre che il Titolare, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, può mettere a disposizione dei propri collaboratori che ne necessitino per il tipo di funzioni svolte, telefoni, telefoni cellulari, computer portatili, tablet e smartphone, ecc., sono state inserite nel Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

## **1. Entrata in vigore del Regolamento e pubblicità**

- 1.1 Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.
- 1.2 Copia del Regolamento, oltre ad essere affisso nella bacheca aziendale anche per quanto prevede l'art.7 della Legge n. 300/1970, verrà consegnato a ciascun dipendente, anche ai fini dell'art. 13 del GDPR 2016/679 e dell'art.4, comma 3°, dello Statuto dei lavoratori, oltre che a collaboratori, consulenti, agenti od altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale il Titolare, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare aziendale.

## **2. Campo di applicazione del Regolamento**

- 2.1 Il nuovo Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti del Titolare a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, agenti di commercio, prestatori d'opera intellettuale, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con quest'ultimi.
- 2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile esterno del trattamento" o "terzo", ai sensi dell'art. 4 comma 10 del GDPR 2016/679, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale od a favore del Titolare stesso.

## **3. Utilizzo del Personal Computer**

- 3.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal

computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

- 3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Titolare solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.
- 3.3 Il Titolare rende noto che il personale incaricato che opera presso il servizio Information Technology (nel seguito per brevità "Servizio IT") della stessa è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Titolare, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio ITC ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.
- 3.4 Il personale incaricato del Servizio IT ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
- 3.5 **Non è consentito** l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio IT per conto del Titolare né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone il Titolare a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico del Titolare, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.
- 3.6 Salvo preventiva espressa autorizzazione del personale del Servizio IT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).
- 3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio IT nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.
- 3.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

#### **4. Gestione e assegnazione delle credenziali di autenticazione**

- 4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio IT, previa espressa indicazione della Direzione aziendale ovvero previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
- 4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio IT, associato ad una parola chiave (password) riservata che dovrà venir **custodita dall'incaricato con la massima diligenza e non divulgata**. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio IT.
- 4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- 4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici). [OPZIONE: Il sistema assegna di default un termine di validità delle password: qualora l'utente non

provveda a variare la propria password in tempo, l'accesso al personale computer e/o al sistema verrà temporaneamente bloccato.]

- 4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio IT.
- 4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del Servizio IT del Titolare .

## 5. Utilizzo della rete informatica

- 5.1 Per l'accesso alla rete del Titolare ciascun utente deve utilizzare la propria credenziale di autenticazione.
- 5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- 5.3 Le cartelle utenti presenti nei server del Titolare sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del Servizio IT. (*Eventuale*: Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato del Servizio IT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente).
- 5.4 Il personale del Servizio IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
- 5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.
- 5.6 Nella gestione dei sistemi informatici aziendali, il servizio IT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto 12.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3.3., e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

## 6. Utilizzo di altri dispositivi elettronici

- 6.1 **Tutti i dispositivi elettronici dati in dotazione al personale del Titolare devono considerarsi strumenti di lavoro:** ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni aziendali, PC portatili, tablet, telefoni cellulari, smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete del Titolare o di condividere documenti, dati e materiali ivi conservati e/o trattati.
- 6.2 L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura del Servizio IT per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente avvisare il Titolare servizio IT, e comunque al massimo entro 24 ore dal fatto.
- 6.3 Con riferimento ai telefoni aziendali e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del Servizio IT.

- 6.4 Si precisa, peraltro, che le disposizioni previste nel presente Regolamento ai punti 3, 7, 8, 9, 10 e 11 dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.
- 6.5 Viene infine disposto il divieto di utilizzo per fini personali di fax aziendali, per spedire o per ricevere documentazione, e/o di fotocopiatrici aziendali, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

## 7. Utilizzo e conservazione dei supporti rimovibili

- 7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- 7.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
- 7.3 Viene severamente vietato l'utilizzo di supporti rimovibili personali.
- 7.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio IT e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del Servizio IT.

## 8. Uso della posta elettronica

- 8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- 8.2 È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
  - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
  - la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
- 8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza commerciale e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l'attività aziendale e non utili alle esigenze aziendali, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dal Titolare quale corrispondenza e documentazione lavorativa e non personale.
- 8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogha dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.
- 8.5 Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che i messaggi ivi contenuti, avendo presuntivamente natura di corrispondenza commerciale, verranno conservati nei server aziendali a norma dell'art. 2220 del Codice civile per un periodo congruo alle finalità aziendali e non oltre ad anni 10.
- 8.6 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

- 8.7 È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
- 8.8 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata e disattivata dall'utente.
- 8.9 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura del Servizio IT.
- 8.10 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dal Titolare, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 8.8).
- 8.11 Il personale del Servizio IT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.
- 8.12 Il Titolare si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l'utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.
- 8.13 La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Il Titolare si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità aziendale; in tal caso:
- avranno accesso alla casella esclusivamente dipendenti individuati dal Titolare in funzione alle mansioni lavorative assegnate;
  - verranno inviate mail ai mittenti con indicazione della diversa casella di posta elettronica aziendale cui trasmettete i messaggi;
  - viene escluso, comunque, l'invio di messaggi da tale casella di posta.
- 8.14 Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di cui il Titolare si fosse dotato, tale utente dovrà attenersi alle regole previste nell'ulteriore apposito Regolamento aziendale a ciò dedicato e che va comunque a completare ed integrare il presente Regolamento.

## 9. Navigazione in Internet

- 9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.** È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
- 9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet per:**
- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio IT);
  - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o del Servizio IT) e comunque nel rispetto delle normali procedure di acquisto;
  - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
  - la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
  - l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

- 9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, Il Titolare rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".
- 9.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio IT ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Titolare.
- 9.5 L'utilizzo di tutte le reti WiFi presenti presso il Titolare è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal reparto IT.
- 9.6 L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.
- 9.7 L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono svolti controlli automatici che impediscono l'accesso utilizzando dispositivi non abilitati.

## **10. Protezione antivirus**

- 10.1 Il sistema informatico del Titolare è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
- 10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio IT.
- 10.3 Ogni dispositivo magnetico di provenienza esterna al Titolare dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio IT.

## **11. Partecipazioni a social media**

- 11.1 L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, LinkedIn™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dal Titolare attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 9.2).
- 11.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, il Titolare ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti dello stesso Titolare.
- 11.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dal Titolare riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partners del Titolare stesso. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che del Titolare; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi del Titolare, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale del Titolare.
- 11.4 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Responsabile d'ufficio.

- 11.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso il Titolare, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.
- 11.6 Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Responsabile d'ufficio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con il Titolare, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili al Titolare.

## **12. Osservanza delle disposizioni in materia di Privacy**

- 12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati/soggetto terzo .
- 12.2 Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 13, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 14), fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).
- 12.3 Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, il Titolare provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

## **13. Accesso ai dati trattati dall'utente**

- 13.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti 3.3. e 3.4, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

## **14. Sistemi di controlli graduali**

- 14.1 In caso di anomalie, il personale incaricato del servizio IT effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
- 14.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## **15. Sanzioni**

- 15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni di

cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

## **16. Aggiornamento e revisione**

- 16.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale.
- 16.2 Il presente Regolamento è soggetto periodicamente a revisione.

Il Titolare del trattamento  
Anna Rachele Donnici  
Firma autografa sostituita a mezzo stampa  
ai sensi dell'art.3 comma 2 del D.Lgs. 39/93